**AFRL-IF-RS-TR-2005-142**
**Final Technical Report**
**April 2005**


# ADVANCED COURSE IN ENGINEERING (ACE)

**Syracuse University**



**AIR FORCE RESEARCH LABORATORY**
**INFORMATION DIRECTORATE**
**ROME RESEARCH SITE**
**ROME, NEW YORK**

**STINFO FINAL REPORT**

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2005-142 has been reviewed and is approved for publication

APPROVED: /s/
DANIEL NERENBERG, LT, USAF
Project Engineer

FOR THE DIRECTOR: /s/
WARREN H. DEBANY, JR.
Technical Advisor
Information Grid Division
Information Directorate

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 074-0188*



| 1. AGENCY USE ONLY (Leave blank) | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| | April 2005 | **Final** **Jul 03 – Apr 04** |

**4. TITLE AND SUBTITLE**

ADVANCED COURSE IN ENGINEERING (ACE)

**5. FUNDING NUMBERS**

G - FA8750-04-1-0208
PE - 65502F
PR - GRIF
TA - 00
WU - 01

**6. AUTHOR(S)**

Kamal Jabbour

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Syracuse University
Office of Sponsored Programs
113 Bowne Hall
Syracuse NY 13244-1200

**8. PERFORMING ORGANIZATION REPORT NUMBER**

N/A

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

AFRL/IFGB
525 Brooks Road
Rome NY 13441-4505

**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

AFRL-IF-RS-TR-2005-142

**11. SUPPLEMENTARY NOTES**

AFRL Project Engineer: Daniel Nerenberg, Lt, USAF/IFGB/(315) 330-2417 Daniel.Nerenberg@rl.af.mil

**12a. DISTRIBUTION / AVAILABILITY STATEMENT**

*APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.*

**12b. DISTRIBUTION CODE**

**13. ABSTRACT** ***(Maximum 200 Words)***

Syracuse University completed the requirements for this grant and successfully delivered a turn-key summer Advanced Course in Engineering on Cyber Security at the Rome Research Site. They recruited and selected students, developed the curriculum, hired the faculty, delivered the instruction and evaluated the students. In addition, we placed the students in internship at the lab and affiliated contractors, where they worked on projects related to cyber security challenges of Homeland Security.

**14. SUBJECT TERMS**

Cyber Security, ACE (Advanced Course in Engineering)

**15. NUMBER OF PAGES** 38

**16. PRICE CODE**

| 17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE | 19. SECURITY CLASSIFICATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
|---|---|---|---|
| UNCLASSIFIED | UNCLASSIFIED | UNCLASSIFIED | UL |

# Table of Contents



# List of Appendixes

## Executive Summary

We delivered successfully the Advanced Course in Engineering on Cyber Security (ACE) to twenty-six (26) students during the summer 2004. The majority of the students attended college pre-commissioning reserve officer training programs at various institutions around the country. The ACE also included a pilot program with two local high-school students.

The ACE sought to develop the next-generation cyber security leaders from the best students at US colleges and universities. It targeted the top students in computer-related disciplines. The course taught them to become original thinkers, problem solvers and technical leaders.

The ACE achieved its stated objectives through focused instruction with strong emphasis on problem solving. Faced with real-world problems, the ACE faculty taught the students to formulate clear problem statements, make reasonable assumptions, apply engineering tools and techniques, solve the problems to a certain depth, apply risk analysis to the solutions, and deliver those solutions on time. In addition to solving problems and delivering solutions on time, students learned to communicate through written reports and compelling presentations.

Taught under the auspices of the Griffiss Institute in Rome, the ACE partnership included Syracuse University, the US Military Academy at West Point, and the Information Directorate at the Air Force Research Laboratory. The faculty was drawn from academia, government and industry, and provided the students with broad cyber security experiences. The course met for ten weeks between 3 June and 13 August 2004, enabling students to earn four academic credits applicable towards their degree of study, and satisfied the requirement of cooperative work experience for several students.

Besides teaching a broad curriculum on cyber security, the ACE placed the students with AFRL where they contributed their new-found knowledge to ongoing research and development projects. A capstone Hackfest also permitted the students as well as AFRL personnel to put into practice many of the lessons learned in the course, to test state-of-the-art tools, and to gather data for use in ongoing activities.

# 1. Technical Approach

## *1.1 Technical Discussion*

In his introduction of **The National Strategy to Secure Cyberspace**, President George W. Bush wrote that "securing cyberspace is an extraordinarily difficult strategic challenge that requires coordinated and focused effort from our entire society" and that "the cornerstone of America's cyberspace security strategy is a public-private partnership."

The Advanced Course in Engineering on Cyber Security (ACE) addressed one component of the National Strategy to Secure Cyberspace by developing the top college students into the next generation of cyber security leaders. Through a public-private partnership among the Air Force Research Laboratory, the US Military Academy and Syracuse University, the ACE followed the proven model of the General Electric Advanced Course in Engineering – formerly known as the Edison course – to transform students into original thinkers, problem solvers and technical leaders.

Far from creating another computer security training program, the pedagogical philosophy underlying the ACE sought to develop leadership skills through problem solving and technical excellence. The following paradigm summarizes best this philosophy: faced with a real-world problem, the graduates of the ACE demonstrated the ability to:

1. formulate a clear problem statement,
2. make reasonable assumptions,
3. apply sound analytical techniques and engineering tools,
4. solve the problem to a certain depth,
5. perform risk analysis on the solution, and
6. deliver a solution on time.

This mindset of an engineering leader was best described by Gene Kranz in his book "Failure is not an Option." As director of NASA's mission control in the Apollo era, Kranz led his engineers into uncharted territory, the Moon's, and established our unchallenged leadership of space.

Cyberspace in the twenty-first century proves no less challenging than outer space in the twentieth century, and our national security relies on establishing and maintaining unchallenged leadership in cyberspace. The ACE develops cyber security leaders by selecting the top college students in US colleges, providing them with one-on-one mentoring by nationally recognized cyber security leaders from academia, industry and government, and educating them to solve real-world problems in cyber security.

The inaugural offering of the ACE in summer 2003 graduated seventeen (17) students from the following institutions:

- Baylor University,
- University at Buffalo,
- University of Colorado,
- Embry-Riddle Aeronautical University ,
- Georgetown University,
- Michigan Institute of Technology,
- North Carolina State University,
- University of Notre Dame,
- Pennsylvania State University,
- Rochester Institute of Technology,
- Syracuse University, and
- Washington State University.

The 2004 ACE students graduated from the following institutions:

- University of Portland — Air Force ROTC
- Syracuse University — Civilian undergraduate
- Virginia Inst of Tech. — Air Force ROTC
- Michigan Tech U — Air Force ROTC
- Texas A&M — Air Force ROTC
- Michigan State U — Air Force ROTC
- University at Buffalo — Civilian graduate student

- University at Buffalo Civilian undergraduate
- Oklahoma State U Air Force ROTC
- Michigan Tech U Civilian undergraduate
- Purdue University Air Force ROTC
- Rochester Inst of Tech Civilian undergraduate
- University of Utah Air Force ROTC
- Illinois Inst of Tech Air Force ROTC
- Rochester Inst of Tech Air Force ROTC
- Michigan Tech U Civilian undergraduate
- Florida State U Air Force ROTC
- Syracuse University NSF SFS cyber fellow - graduate
- Valdosta State U Air Force ROTC
- Embry Riddle Aero U Air Force ROTC
- Embry Riddle Aero U Army ROTC
- Embry Riddle Aero U Army ROTC
- Cornell University Navy ROTC

In addition, underclassmen and high school students audited the course from the following institutions:

- Syracuse University Air Force ROTC
- Syracuse University Air Force ROTC
- Rome Free Academy Air Force Jr. ROTC
- Rome Free Academy Air Force Jr. ROTC

### *1.2 Technical Program Summary*

The ACE sought to develop the college students into cyber security leaders through a three-pronged approach:

1. developing problem solving skills and on-time performance,

2. communication through sound technical writing and compelling presentations, and
3. mentoring by experienced cyber security professionals.

The rhetorical question on whether leaders are born or developed may be answered by looking at a four-minute miler. While genetics play a pivotal role in breaking the four-minute barrier, it takes years of hard training to prepare for the feat. Similarly, by starting with college students committed to serving this Nation and who have demonstrated leadership qualities, and by equipping them with the tools to solve a series of real-world problems of increasing complexity, we set-up for success in transforming them into the next generation of cyber warriors.

Effective communication is arguably a distinguishing trait of a leader. Therefore, the ACE focused on developing the students into effective communicators by requiring individual weekly written reports, and several structured team presentations. The instructors and the ACE director evaluated student reports and the presentations, and provided detailed feedback and constructive criticism. Appendix A-1 contains a sample student report, and Appendix A-2 contains a writing guide and a grading template.

The course met once a week for a full day on Mondays. A typical class started with the timely submission of written reports and the oral presentation of solutions for the previous week's problem. Students discussed their solutions with the ACE Director and the instructor, before moving on to a new problem. Each week brought a different instructor, who assigned a substantial real-world problem, then lectured for six hours on the background material for that topic.

The ACE carried four credit hours of academic credit from Syracuse University. Successful completion of the all course assignments permitted the students to apply the earned credit towards their programs of study at their host institution.

Finally, students were assigned to work with mentors at local private or government cyber security laboratories. This mentoring relationship exposed the students to practical challenges of cyber security, and permitted them to establish professional relationships with domain experts.

**Outline and Schedule**

The duration of the ACE was ten weeks during the June-August timeframe. Each week focused on one area of cyber security as detailed below:

1. Legal Issues: Internet laws and cyber crime, the Fourth Amendment of the US Constitution, search and seizure of data, rights and privacy issues, government versus private workplace, search warrants and wiretap laws, the Patriot's Act.
2. Security Policies: establishing and implementing security policies, confidentiality integrity and availability considerations, identifying vulnerabilities and threats, establishing disaster response and recovery procedures.
3. Cryptography: mathematical basis for data encryption, substitution ciphers and the Data Encryption Standard, private-key and public-key cryptography, key distribution and trusted authority, digital signatures.
4. Computer Security: operating systems and file system security, passwords and one-way hashes, user-space administration, archiving and back-up strategy, intrusion detection, disaster response and recovery.
5. Digital Forensics: procuring and analyzing digital evidence, preserving the chain of custody of digital evidence, recovering hidden data on hard drives, classifying file systems, analyzing slack and sector data, recovering lost clusters.
6. Network Security: TCP-IP packet format and vulnerabilities, protocol and implementation flaws, buffer overflow, denial-of-service attacks, distributed attacks, email, domain name system, web servers.
7. Network Defense: host and network security, firewalls and periphery intrusion detection systems, bastion hosts, network monitors and traffic analyzers, network logfiles, detecting anomalous behavior, network recovery.
8. Network Attack: port scanners and packet sniffers, IP spoofing, identifying vulnerabilities, designing and implementing network attacks, engineering malicious code, worms and viruses, offensive cyber warfare.
9. Steganography: data hiding in images, classifying steganography algorithms and tools, categorizing vessel capacity, detection and recovery of hidden data, digital watermarking, streaming media steganography, multilingual steganography.

10. Next-Generation Cyber Security: wireless local area networks, wireless encryption protocols, Next-Generation Internet Protocols IPv6, embedded systems, 3G cell phones and personal data assistants.

For each topic, the instructor in charge assigned a substantial real-world problem that required 40 to 80 hours of team work to solve. Students worked on teams of three to solve each problem, then wrote and submitted individual reports.

# 2. Special Technical Factors

## *2.1 Facilities and Resources*

The renovation of Building 448 – formerly Air Force barracks – permitted housing the students on Griffiss Park. This convenience provided added flexibility to the course, including in-site classroom and laboratory space, and overall a community environment.

The majority of classes were held in the Quad Room in Building 3, providing convenient access to AFRL facilities and laboratories.

## *2.2 Faculty and Staff*

The following constituted the faculty of the 2004 ACE:

- Dr. Steve Chapin – Syracuse University
- Dr. Shiu-Kai Chin – Syracuse University
- Maj Ronald Dodge - USMA
- Dr. Heather Dussault – SUNY IT
- Joseph Giordano – AFRL/IF
- Chet Hosmer – Wetstone Technologies
- Dr Kamal Jabbour – ACE Director
- Lt Chad Korosec – USNR

- Dr. Daniel J. Pease, Syracuse University
- Dr. Leonard Popyack – AFRL/IF
- Lt Col Daniel Ragsdale - USMA
- Paul Ratazzi – AFRL/IF

On October 15, 2004, Dr. Susan Older assumed the role of principal investigator on this project, replacing Dr Kamal Jabbour who had accepted a part-time career position with the US Air Force Research Laboratory Information Directorate.

### *2.3 Reporting*

The ACE staff presented and discussed the curricular data at a meeting of the ACE faculty on 3 September 2004, and subsequently traveled to various constituents to discuss the results.

ACE staff visits included Purdue University, Texas A&M, Pennsylvania State University, University of Norwich, among others, where we met with AFROTC cadre and cadets to present results of the 2004 ACE.

Extensive communication and correspondence with AFROTC/CC also followed, aimed at designating the ACE as a sanctioned professional development training (PDT) opportunity.

The results from the 2004 ACE were also presented to the Dr. Diana Gant, National Science Foundation program manager for the Scholarship for Service program, since two SFS fellows had taken the ACE.

## 3. Conclusions

Syracuse University completed the requirements for this grant, and successfully delivered a turn-key summer Advanced Course in Engineering on Cyber Security at the Rome Research Site. We recruited and selected students, developed the curriculum, hired the faculty, delivered the instruction and evaluated the students. In addition, we placed the students in internship at the lab and affiliated contractors, where they worked on projects related to cyber security challenges of Homeland Security.

## Appendix A-1 Sample Student Report

**Appendix A-1, which includes Appendixes A through C, was submitted by the students and appears as written. Typographical and administrative errors, therefore, have not been changed in an effort to maintain the integrity of the document.**

# ADVANCED COURSE IN ENGINEERING

# 2004 Cyber Security BOOT CAMP

Modification of Air Tasking Orders

for Joint Operations

**By**

**Team Alpha**

**June 28, 2003**

**Gavin Littleboy, Jerry Conner and Sara Haydanek**

## Executive Summary

The problem necessitates the modification of air tasking orders to provide secure, fast communication. The orders must fit the needs of the air force, the navy, and ground forces. The orders must also handle the cooperation of the services as one team. The problem requires the specification of all subjects, objects and operations on the objects. The problem also entails the organization of the subjects into the specified roles and an explanation as to how identification and authentication of these roles succeeds.

We assume that the government accepts the requirement of a minimum of five years setup time for this organization. We also assume that aircraft carriers provide guidance from the navy for the airplanes. We also assume that during a wartime situation there is a streamlined form of communication that goes against standard procedures.

The system must succeed in the provision of secure, fast communication that provides reliable information. Threats to this system include communication failure, packet sniffing and impersonations. To answer these threats the organization uses encryption, visual confirmation and certificates. The subjects of the system consist of commanders, pilots and the armed services. The objects include directions, guidance and electronics. The operations on these objects involve bombing, flying and giving orders. The use of quantum key encryption, certificates and digital signatures ensure a secure transfer of information. The use of encryption, digital signatures and reference monitors make certain the verification and authorization of authority. These tools also ensure the verification of guidance from the navy and the request for an air strike.

### 1.0 Problem Statement

The problem necessitates the modification of air tasking orders to provide secure, fast and reliable communication. The orders must fit the needs of the air force, the navy, and ground forces in cooperation with one another. The problem necessitates the consideration of threats to the system, and required solutions to the threats. The problem requires the specification of all subjects, objects and operations on the objects. The problem also entails the organization of the subjects into the specified roles and an explanation as to how identification and authentication of these roles succeeds. The problem requires establishment of the integrity of the system created. The problem entails the explanation of the management of cryptographic key distribution and how the keys are established and maintained. The assignment needs trust networks created and a display of the certification authorities needed.

## 2.0 Background

Secure transmissions require techniques that ensure the identification of the sender and the integrity of the file. Asymmetric key cryptography provides the tools needed for secure transmissions. [2] The use of public and private keys allows only those users with the correct keys to view a message and authenticate its origin. Encryption and decryption slow down the passage of information but the added security makes it a worthwhile compromise. Encryption provides no help for the initial distribution of keys since the receiver possesses no key. This leaves susceptibility in the transmission of private keys. Quantum key distribution gives the necessary security in key distribution. The use of individual photons ensures the privacy of a transmission. The uncertainty principle of physics shows that reading a photon changes its state. [1] This state change allows the receiver to determine whether an outside party read any transmitted photons. The use of these principles provides a secure technique for key distribution.

Wartime communication for the US traditionally falls short of expectations for joint operations. Each branch faces challenges in protocol, secure lines, and chain of command. [4] The need for one commander arose in desert storm and continues to improve in design today. The use of a unified commander to run the battlefield allows information to flow up the chain and orders to flow down the chain in a timely manner.

Military targets of opportunity often include close air support or interdiction. [5] The need for a ground soldier to call for air strikes during battle often requires nearby aircraft to modify their air tasking orders. Air tasking orders often take up to forty-eight hours to prepare. [4] Streamlined communication during wartime operations allows joint commanders to make quick decisions about the battlefield and give secure air tasking orders within minutes of a decision.

## 3.0 Assumptions

### 3.1 Technology

The solution presented includes innovative technology. The use of quantum key distribution requires items not readily available on the market today. Tested models exist today and a fair estimate for availability estimates to five

years. We assume the secure communication plan for the military presented in this paper faces five years of discussion before implementation.

### 3.2 Chain of Command

We assume wartime lines of communication for the infrastructure presented here. Time sensitive information must traverse the chain of command quickly for effective results. The assumption that unit commanders represent the communication between theater command and the troops allows for the quick and secure flow of information.

### 3.3 Navigation

We assume naval navigation comes from an aircraft carrier. The choice of subjects for our organization chart required us to decide from where the guidance arrives. We choose aircraft carriers because they posses the capabilities required to direct air traffic.

## 4.0 Techniques and Tools

The problem required the use of class notes and the AFRL Technical Library. The class notes introduced the subject matter. The AFRL Technical Library allowed us further research into the topics required for this assignment.

## 5.0 Problem Solution

### 5.1.1 System Goals

The system must provide secure, fast communication. It must not allow the enemies to intercept or change the commands, and at the same time it must allow commanders to send and receive commands in minutes. The system requires flexible hardware and tactics so that it succeeds in times of stressful warfare. The system must also provide reliable information at all times.

### 5.1.2 Threats to Security

Enemies threaten the security of secret warfare information. One way in which enemies endanger the system is through packet sniffing. Enemies can grab packets and use the information they find to harm the United States. Enemies also cause global positioning system jams to prevent the transfer of important information. Enemies

electronically impersonate allies as well. Enemies attempt to alter information sent electronically to force the receiver to change the commands. Communication failure in general is a major threat to the system.

Solutions to these threats include encryption, certificates and reference monitors. A secure encryption decreases the possibility that an enemy can alter or read the commands sent electronically. Certificates authenticate the user and maintain a trust network. Reference monitors stop users unable to complete specified electronic commands and act as a guard for the operations. Visual monitors on the air force planes provide another way of authentication. The pilot can visually watch his commander give him an order and thus prove the truth of the command. Electronic command confirmations complete with digital signatures also provide verification and authority. The use of confirmation receipts ensures that no communication failure has occurred. The confirmation receipts use certificates to show that the correct receiver got the message.

### 5.2.1 System Subjects

At the highest level, subjects in the system include the director of joint command and control communications and the unified commander. These subjects communicate laterally with each other. The director of joint command and control communications funnels necessary intelligence toward the unified commander, and the unified commander uses this information to determine the best course in terms of operations within his theater of operation.

The unified commander sends orders down the chain of command through his component commanders. These component commanders lead operations for their respective military branches. For instance, the air component commander directs all air operations within his theater.

Component commanders communicate further down the chain of command to unit commanders. These unit commanders direct the actions of the deployable units in their charge. For instance, the wing commander assumes responsibility for and directs the actions of his wing.

Several roles comprise the lowest level of the chain of command hierarchy. The lowest level of the chain of command in the army consists of individual soldiers. In the navy, our interest lies in the navigators that must direct our pilots. Finally, the air force hierarchy ends with the pilots.

### 5.2.2 System Objects

We must act on many objects to implement a secure system that issues and modifies air tasking orders to aircraft already in flight successfully. These objects include aircraft, ships, bombs, targets, orders, and intelligence information.

Some of these objects we must attach to specific units or branches. For instance, the air force must take charge of aircraft used in the theater of operation. Further, the navy must control the ships. However, ownership of these objects does not imply that other subjects may not act upon these objects. For example, aircraft require the navigational guidance that the navy must provide. In this manner, the navy acts on aircraft despite air force ownership of these aircraft.

### 5.2.3 System Operations

Many operations exist for each object, and permissions that allow subjects to perform those operations vary dependant upon the role of each subject. For instance, many subjects may issue orders. These subjects include unified commanders, component commanders, and unit commanders. By contrast, lower echelon units such as soldiers, pilots, and navigators may only receive and execute orders. Furthermore, unit and component commanders may receive orders from the unified commander. Only the unified commander may change orders or approve orders suggested from lower echelons.

Based on the intelligence gathered at the joint command and control center, the director of joint command and control communications may advise the theater commander of important targets in his theater of operation. From the opposite end of the hierarchy, soldiers may advise their commanders of targets in their immediate area. Final authority in target selection rests with the unified commander.

The director of joint command and control communications may further advise the theater commander on the use of military assets in his theater of operation. These assets include aircraft, ships, and bombs. Only pilots may fly aircraft, but these pilots rely on the navigational guidance provided by the navy. Further, pilots may bomb approved targets, and soldiers may request targets be bombed.

Finally, all subjects may receive intelligence information. However, only the director of joint command and control communications may distribute this information. Other subjects must convince the joint command and control center of their "need to know" before the joint command and control center may pass along such information.

### 5.3.1 Organization of Principals into Roles

See Appendix A

### 5.3.2 Principal Identification

Digital signatures provide the necessary requirements for identification and authentication. A digital signature allows the recipient of information to determine from whom the information came. In the operations of the given assignment, individuals must decipher the sender of a received message. The trust network consists of a tree diagram of certifications. For the initial request of airpower, an Army soldier calls up the chain with their digital signature from a secure phone. The unified commander recognizes the digital signature and implements their commands down to each respective service. These services recognize the unified commander's digital signature and propagate the information down to the pilot and navigator. The pilot and navigator confirm the digital signature of the unified commander and carryout the orders. During the operation, the navigator communicates with the pilot with the use of their digital signature. The pilot recognizes this signature from the established trust network and follows their guidance. The certification tree organizes subjects by their roles. This allows the receivers of information to understand where the information comes from and carryout the necessary orders.

### 5.3.3 Information Integrity and Authentication

The integrity of a signal depends on the corruption of information through data transfer errors or possible malicious attacks on the signal. Asymmetric key cryptography employs the use of public and private keys to encrypt

distributed information. Given that private keys remain secure, asymmetric key cryptography allows users secure and reliable transmission of information. Errors in transmission cause a decrypted file to lose its meaning. To acquire the data requires a new transmission. Malicious attacks on the signal results in the same problem. Modification of a transmitted file causes the decryption to reveal erroneous data. The use of 256-bit keys to secure information protects against an adversaries ability to modify a given set of information in a readable form. Modification requires access to the private key of the sender. This process results in a digital signature, which ensures the recipient of the message knows where it originated. The comparison of a hash of the received file with that of the original ensures the file maintained its integrity. The techniques of asymmetric keys, digital signatures and hash comparisons determines whether an air tasking order, request for air strike or navigational guidance posses integrity and confidentiality.

### 5.3.4 Key Distribution

The distribution of cryptographic keys must support security and the ability to respond in real time. The use of quantum key distribution ensures security through the laws of physics. The use of key pads that run continuously allows for the transmission of time sensitive data in real time. The technology of quantum key distribution allows the military to operate with confidence in times of war and peace.

The security of quantum key distribution relies on the theorems of quantum physics. The intrinsic randomness of quantum physics allows the production of unbreakable keys. We cannot mathematically describe keys that possess no order. This lack of order prevents the discovery of the key by mathematicians who may exploit the transmitted data. The threat of an outside subject that intercepts the signal also has no bearing on the security of the key. Heisenberg's uncertainty principle discusses the fact that the mere observation of a system perturbs it in an irreparable way. Quantum key distribution deals with the transmission and detection of single photons. Physics shows an observer cannot read or capture the photon and preserve its state. In quantum key distributions, the state of a photon determines the value of the bit. Polarization techniques used in the transmission of data photons reveals whether an observer was present in the transmission. The random nature of quantum particles combined with uncertainty principle allows for a standard in key distribution never seen before.

Real time response requires keys to be available to all subjects that transmit data at all times. Fiber optics or satellite communications distribute quantum keys. Fiber optics limits distribution to physically connected sources. Transmissions that covers over seventy kilometers require multiple Alice and Bob chains to keep the information secure. Satellite communication allows for wide dispersion of secure keys. The first few miles of atmosphere produce a significant amount of interference for photons. However, the distribution to aircraft poses no such problem. Lost bandwidth occurs since ground stations induce more errors in communication. Typical bandwidth allows a 256-bit key to change four times a second. Continuous broadcast of private keys to the aircraft and ground station and storage capacities at each allow for secure communication for extended periods, much longer than typical missions requirements. Weather plays a vital role in satellite communication, but with the storage of the distributed keys secure communication continues.

### 5.3.5 Certification Authorities

See Appendix B

### 5.4.1 Authority

A policy created by the organization defines authority. It specifies the requirements and purpose of the job. Individuals may gain authority by appointed of superiors. Individuals may also gain authority as part of the policy. For example, if the president suddenly steps down the vice president gains the authority of president. The citizens may also elect upper levels of authority. Private key certificates provide verification and authentication of authority. Digital Signatures and reference monitors also ensure the verification and authentication of authority.

### 5.4.2 Requests for Air Strikes

Encryption, reference monitors and access codes provide verification and authentication of air strikes. The use of private keys through encryption verifies that the information received is correct. Reference monitors ensure that only those with appropriate clearance access certain electronic commands and operations. Access codes given each day to the commanders verify the authority of those on the field. The commanders on the field read the access code to theater commander to authenticate the request. Voice recognition provides another level of verification of

authority. Verification of requests from the Joint Operations Command intelligence center proves the reliability of requests from the ground.

#### 5.4.3 The Order of Air Strikes

Digital signatures, certificates and encryption provide verification and authentication of the authority to order air strikes. Digital signatures and certificates that use private keys ensure that the information sent is from a proper authority. The use of strong encryption ensures that only those with proper clearance gain access to the information. Reference monitors guarantee that only those with the proper authority acquire access to the specified electronic information and operations. Visual monitors onboard the planes provide both visual and voice confirmation of the authority of the commander. The visual monitors and electronic systems installed on the planes provide two solid forms of authentication.

#### 5.4.4 Guidance

Encryption, digital signatures and certificates provide verification and authentication of the navigation provided by the navy. The use of encryption ensures that the enemies cannot steal the information. Digital signatures and certificates ensure that the navy is the sender of the guidance. Reference monitors guarantee that only those with the required clearance provide the navigation to the air force pilots.

### 5.5 Logical Analysis

See Appendix C

## 6.0 Risk Assessment

### 6.1 Technology

The assumption that the technology required to implement a quantum key distribution network could prove naive. If a need emerges for the military to change current communications systems immediately then the plan would not be ready. This could compromise the security of military communications.

### 6.2 Chain of Command

The assumption that wartime communication exists could result in poor peacetime communication. Wartime allows streamlined information to deliver bombs on target on time. Peacetime incorporates more levels of command that might break the window of opportunity presented.

### 6.3 Navigation

The assumption that aircraft carriers provide all guidance to the air force may result in unacceptable risk. The assumption may take away needed aircraft carriers from other important missions. Furthermore, the area may not contain required aircraft carriers. This leaves our mission without a key component.

## 7.0 References


[1] Cingria, Rue. id Quantique. 2004. id Quantique SA. 23 June 2004 <http://www.idquantique.com>.

[2] Chin, Shiu-Kai , and Susan Older. "Formal Methods for Assuring Security of Protocols." The Computer Journal 45.1 (2002): 46-54.

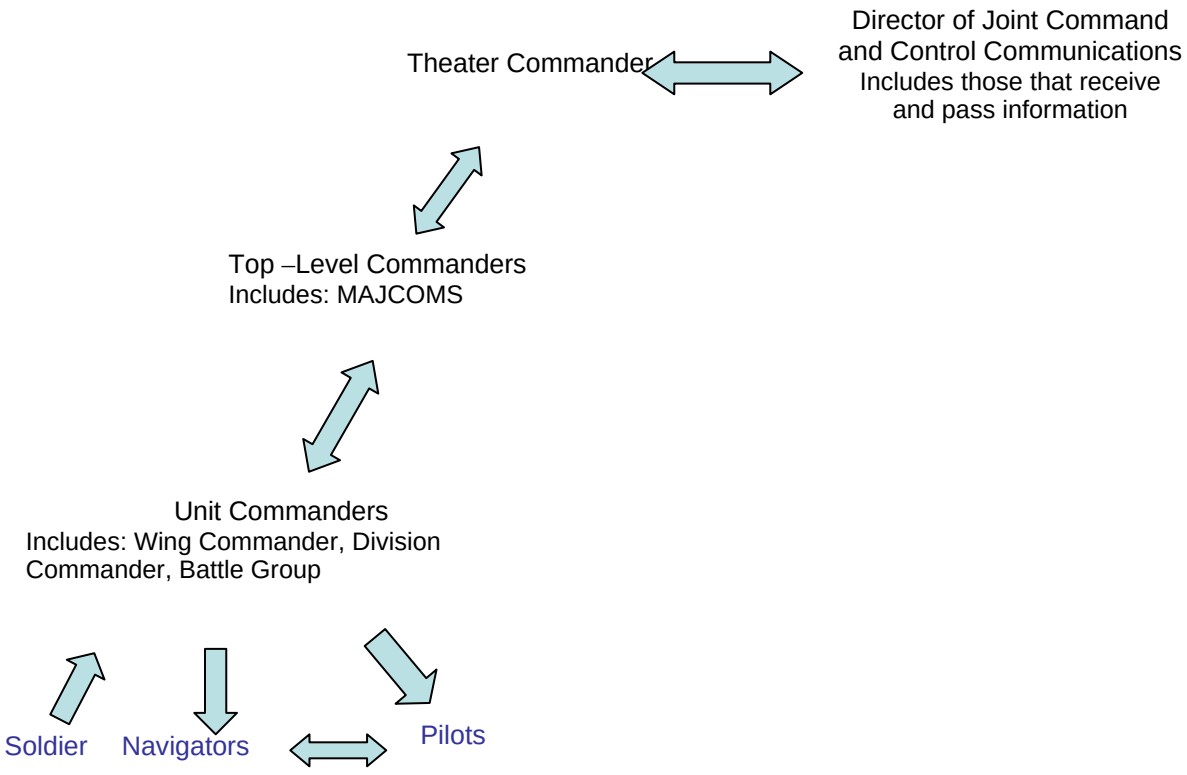
[3] Chin, Shiu-Kai, Polar Humenn, Thumrongsak Kosiyatrakul and Susan Older. “Implementing a Calculus for Distribute Access Control in Higher Order Logic and HOL.” Syracuse: Syracuse University.

[4] Johnson, Dana J., and James A. Winnefeld. Joint Air Operations. Annapolis: Naval Institute Press, 1993.

[5] Warden III, John A. The Air Campaign. Washington: International Defense, 1989.

## Appendix A

# Roles and Subjects



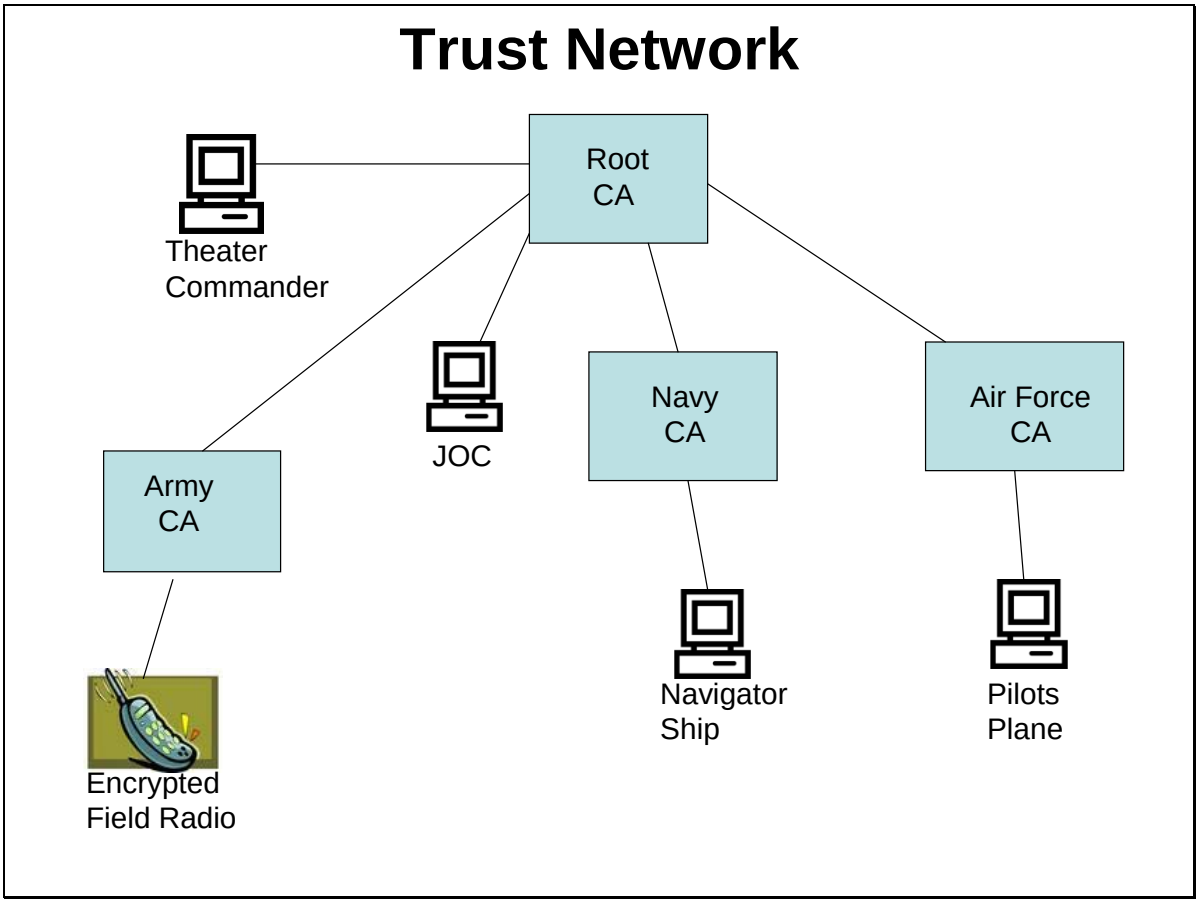
## Operations

- Fly (F)
- Bomb (B)
- Guide (G)
- Command (C)
- Advise (A)
- Request (R)
- Receive Information (RI)
- Give Joint Information (GI)
- Change Orders (CO)
- Receive Orders (RO)

## Access Control Matrix

| **Objects**<br>**Subjects** | **Orders** | **Targets** | **Aircraft** | **Ships** | **Bombs** | **Information** |
|---|---|---|---|---|---|---|
| Soldier | RO | A | | | R , B | |
| Pilot | RO | | F | | B | RI |
| MAJCOMS | C, RO | | | | | RI |
| Theater Commander | C, CO | | | | | RI |
| Unit Commanders | C, RO | | | | | RI |
| Director of JOC | A | A | A | A | A | RI, GI |
| Navigator | RO | | G | | | RI |

## Appendix B


Trust Network
Root CA
Theater Commander
JOC
Navy CA
Air Force CA
Army CA
Navigator Ship
Pilots Plane
Encrypted Field Radio

# Appendix C

### C.1 Validation of Radio Transmission

Consider the scenario in which a soldier requests an air strike. The soldier uses his radio to contact a communications technician at headquarters. To prove the validity of his request, he sends his unit name and authorization code. Based on this, the technician garners two pieces of information.

R says S says m (1.1)

R says (<u,ac> speaks_for S) (1.2)

The technician may only accept the transmission as valid if the Army Certification Authority recognizes the unit and authorization code pair. Thus,

((R ^ $CA_A$) says (<u,ac> speaks_for S)) $\supset$ (R|S) speaks_for (T|S) (1.3)

The $CA_A$ assumes only authorized soldiers possess authorization codes.

$CA_A$ says (<u,ac> speaks_for S) (1.4)

Combining (1.2) and (1.4) yields

(R ^ $CA_A$) says (<u,ac> speaks_for S) (1.5)

We use rule (1.3) to deduce the following.

(R|S) speaks_for (T|S) (1.6)

The monotonic operator, speaks_for, allows us to rewrite this expression as

(R|S) speaks_for (R|S ^ T|S) (1.7)

Thus,

(R|S) speaks_for (R for$_T$ S) (1.8)

Combining (1.1) with (1.8) yields

R for$_T$ S says m (1.9)

### C.2 Relay Request to Higher Authority

The communications technician receives a valid request for an air strike from the soldier. Now, he must relay this request to the air component commander. To do so, he sends a session key through some public key encryption

scheme from his computer to the air component commander. The air component commander now knows two pieces of information

$C_e$ says T says $m_x$ (2.1)

$C_e$ says ($K_T$ speaks for T) (2.2)

The air component commander may only accept this transmission as valid if the Air Force Certification Authority recognizes the key the technician sends. However, the technician uses a key provided by the Army Certification Authority. Thus, the Air Force Certification Authority must check with the Joint Certification Authority to verify that the technician sends a key recognized by the Army Certification Authority.

$((C_e \wedge (CA_J \text{ for } CA_{AF}))$ says $(K_T$ speaks for T))

$\supset (C_e|T)$ speaks for $(CC_{air}|T)$ (2.3)

If the Joint Certification Authority approves the use of the key, we say

$(CA_J \text{ for } CA_{AF})$ says $(K_T$ speaks for T) (2.4)

Combining (2.2) with (2.4) yields

$(C_e \wedge (CA_J \text{ for } CA_{AF}))$ says $(K_T$ speaks for T) (2.5)

We use rule (2.3) to deduce the following.

$(C_e|T)$ speaks_for $(CC_{air}|T)$ (2.6)

We may rewrite this expression as

$(C_e|T)$ speaks_for $(C_e|T \wedge CC_{air}|T)$ (2.7)

Thus,

$(C_e|T)$ speaks for $(C_e \text{ for}_{CCair} T)$ (2.8)

Combining (2.1) with (2.8) yields

$C_e \text{ for}_{CCair} T$ says $m_x$ (2.9)

Since the encrypted message sent by the technician simply relays the validated request for air support sent by the soldier, we say

$C_e \text{ for}_{CCair} T$ says $m_x \supset R \text{ for}_T S$ says m (2.10)

In this manner, the air component commander may assume that the receipt of a validated message from his communications technician implies a validated radio transmission from an authorized soldier that requests air support.

### C.3 Recommend Action

Upon receipt of a legitimate request for air support, the air component commander recommends an appropriate response to the unified commander who then either approves the recommendation or provides orders for a different course of action. The unified commander goes through the Joint Certification Authority for validation while the air component commander goes through the Air Force Certification Authority, as stated. Certification between the two authorities presents no problems as the Joint Certification Authority authorizes the Air Force Certification Authority.

The air component commander forwards his recommendation to the unified commander with the use of encryption in the same manner that the technician forwards the initial request to the air component commander. In similar fashion, we may modify the logical scheme above to represent this transaction.

### C.4 Request Additional Intelligence

The unified commander may request further intelligence from the Joint Command and Control Center. The unified commander sends an encrypted request for information to the Joint Command and Control Center, and the Joint Command and Control Center sends an encrypted response that presents the requested information. These transactions takes place in a manner similar to ones already mentioned.

### C.5 Decision

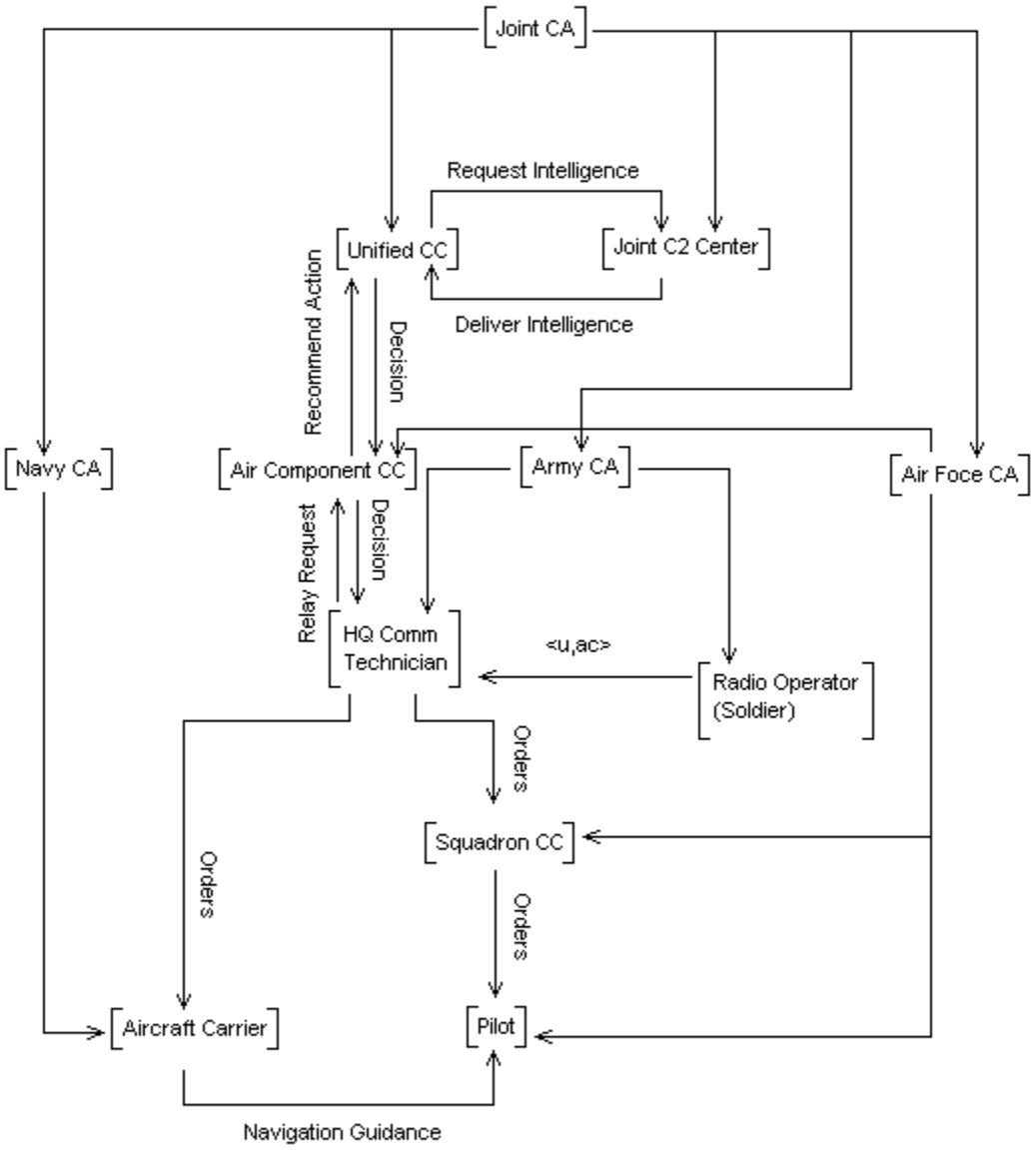
The unified commander decides on the course of action. Either he approves the recommendation brought forth by the air component commander, or he responds with his own directives. These decisions follow the same protocols down the chain as followed up the chain. When the communications technician receives these orders, he then disseminates the orders to the respective air force and navy components. The air force component consists of the

strike aircraft and its associated squadron. The navy component consists of the aircraft carrier, which provides the navigation and guidance for the strike aircraft.

### C.6 Navigation and Payload Delivery

The navy aircraft carrier provides the strike aircraft with navigation and guidance information. This requires secure communications while the strike aircraft proceeds toward its target. The aircraft then bombs the specified target. In this manner, we fulfill the initial request for air support from the soldier. Finally, the pilot reports mission success or failure back to his squadron, which in turn reports to headquarters.

**C.7 Graphical Interpretation**



**C.8 Explanation of Symbols**

| | |
|---|---|
| R | Radio Transmission |
| S | Soldier |
| T | Communications Technician |
| m | Message |
| <u,ac> | <Unit, Authorization Code> |
| $CA_J$ | Joint Certification Authority |
| $CA_A$ | Army Certification Authority |
| $CA_{AF}$ | Air Force Certification Authority |
| $CA_N$ | Navy Certification Authority |
| $C_e$ | Encrypted Computer Message |
| $m_x$ | Encrypted Message |
| CC | Commander |
| C2 | Command and Control |
| K | Key |

**Appendix A-2 Report Writing Guide and Grading Template**

# ADVANCED COURSE IN ENGINEERING
# 2004 Cyber Security BOOT CAMP

# ACE Report Writing Guide

by

Dr Kamal Jabbour

7 June 2004

## 1. Guiding Principles

The ACE writing style seeks to achieve clarity of communication through brevity and simplicity. It promotes short sentences, direct voices and active verbs. It favors past and present tenses over subjunctives. It avoids excessive punctuation, and banishes sentence breaks and sidetracks.

The structure of an ACE report follows the guiding structure of the course. Given a problem, engineers must:

i- formulate a clear problem statement
ii- make reasonable assumptions
iii- apply analytical techniques and computer tools
iv- solve the problem to a certain depth
v- perform risk analysis on the solution, and
vi- deliver the solution on time.

Hence, the ACE report documents the thought process and work effort to solve the problem at hand.

## 2. Report Structure

An ACE report consists of the following parts:

**i-** **Cover Page** – includes the ACE header, an informative title, the name of the author, the name of the team, the names of the members of the team and the date of the report. This writing guide includes a representative cover page.

**ii-** **Executive Summary** – one page long, consists of three paragraphs. The first paragraph states the problem, the second paragraph outlines bounding assumptions, and the third paragraph presents the solution. The executive summary must stand alone as a self-contained document. It may not refer to material in the main body of the report.

**iii-** **Problem Statement –** about one page long, states clearly the problem at hand. It assumes that the reader cannot access the problem statement of the instructor, and presents all the necessary elements of the problem.

**iv-** **Background –** this chapter permits the writer to situate the problem and the solution within the broader field of knowledge. Background information includes reference to prior art and publications, introduces relevant material, and argues the significance of the problem in the broader field of cyber security.

**v-** **Assumptions –** the author states and explains the assumptions that bound the solution space for the problem. The time constraints of the ACE require a problem solution to a certain depth, and often prevent the engineer from delivering an exhaustive, let alone elegant solution. The assumptions seek to bound the problem statement and the solution space to permit a meaningful solution within the allotted time.

**vi-** **Techniques and Tools –** presents the skill set necessary to solve the problem, includes analytical techniques and computer tools. If the problem requires some skills beyond a high school education, the author lists such skills in this chapter.

**vii-** **Problem Solution** – this chapter contains the meat of the report. It presents the solution to the problem, includes procedures and processes, flow charts and diagrams, results and conclusions.

**viii-** **Risk Assessment** – in this short chapter, the author revisits the assumptions, estimates their possible impact on the solution, and identifies potentially catastrophic oversights.

**ix-** **References** – this final chapter includes a list of three-to-five references, showing the name of the authors, document title, publication, date and place of publication.

## 3. Report Format

### 3.1 Construct hierarchy:

A report consists of named chapters (1, 2, 3). A chapter contains titled sections (2.1, 2.2). A section comprises paragraphs. A paragraph connects sentences. A sentence communicates activity.

Within this iterative hierarchy, each element exhibits the ternary structure of actor, act and action. Thus, a sentence communicates the activity of a subject, a verb and an object. A paragraph connects two-to-three sentences to introduce, explain and clarify a thought. A section comprises three or more paragraphs to summarize its content, elaborate on the details, and conclude the thought.

A chapter starts with an introductory section that reviews the previous paragraph and overviews the current chapter, presents material in the middle sections, and concludes with a section that reviews the chapter and previews the next chapter. Finally, a report starts with a preview chapter (formulates a clear problem statement), presents a solution, and concludes with an assessment.

**3.2. A matter of style:**
For consistency and uniformity, we require all reports to use Times New Roman font size 12. You may use bold font and underscoring to highlight section headings. On the cover page, you may use larger fonts for effect.

Use the dotted decimal numbering system for paragraphs and sections. Do not number the Executive Summary. Assign chapter number 1 to the problem statement.

Write your reports on single sided papers, double-spaced lines and one-inch margins on all four sides of the text. Staple the report on the top left corner, and number the pages on the bottom right corner.

Precede a chapter with two blank lines. Precede a section with one blank line. Do not indent or right-justify your paragraphs.

Number sequentially your references, and surround them with square brackets within your text [1]. Do not use footnotes, they belong to the social sciences.

**3.3 A matter of substance:**

Strive to include a subject, a verb and an object in every sentence. If a sentence contains two verbs, separate its parts with a comma. Limit your use of commas to no more than one comma per sentence.

The devil lies in the punctuation. You must use a period at the end of each sentence. You may use a comma to separate two actions within a sentence, or to separate the first two items in a list of three. Do not use colons, semicolons, exclamation marks or question marks.

Strive to maintain sentence integrity. Avoid parentheses and brackets, and do not split two thoughts with a dash.

Do not use apostrophes.

Avoid using quotation marks. Use your own words to cite a reference.

Do not start a sentence with the words *“and”, “but”* or*” because*”. Do not end a sentence with a preposition, such as *“to”, “of”, “in”, “on”, “into”, “onto”, “under”, “over”, “about’, “for”* or *“from”*.

Avoid statements with sweeping categorical adverbs like *“always”, “never”, “any”, “every”, “all”* and *“none”*. They can be disproved easily, and undermine the credibility of an entire report.

Use with care quantitative adverbs like *“few”, “some”, “many”* and *“most”*.

Do not sell yourself short. Do not describe your work as *“easy”, “simple”, “straight forward”, “trivial” or “elementary”* (unless your last name is Holmes).

**3.4 Verbs rule:**

Use active voice verbs only, not passive voice. Attribute clearly the responsibility for action and thought.

Use the first or third persons, but avoid the second person.

Use present tense or past tense only. Do not use future or composite past, subjunctive or conjunctive.

Do not mix tenses in the same paragraph, let alone in the same sentence. Use the present tense to describe activity, and use the past tense to report data and facts.

Do not use continuous action tense and verbs that end with *"ing."* Avoid adjectives that end with *"ly."*

Avoid weak verbs *"be", "have", "can" or "do"*. Use verbs that describe state and action.

Do not use "c*ould", "would" or "should."* Use *"must"* to describe a policy or a requirement.

**3.5 The bottom line:**

Use a spell checker and a grammar checker. Seek readability. For example:

The sentence *"Be."* scored 100% on readability and a grade level 0.

The sentence *"Existentialism provided unsatisfactory explanations."* scored 0% on readability and a grade level 12.

## 4. Presentation Format

Use Microsoft PowerPoint to present your work.

Use Arial yellow, font size 48, for slide titles, and Arial white, font size 32, for the text. Use a navy blue background.

Limit your material to no more than 7 lines per slide.

Aim to balance slide content between concise bullets and runaway sentences.

Avoid tables, equations and quotations. Use charts when appropriate.

# ADVANCED COURSE IN ENGINEERING
# 2004 Cyber Security BOOT CAMP

# Grading Template

Student Names: _____

Team: A B C D E F G H

Lecturer: _____

Lecture Topic: _____

Lecture Date: _____

| | | |
|---|---|---|
| Cover Page | /10 | |
| Executive Summary | /10 | |
| Problem Statement | /10 | |
| Background | /10 | |
| Assumptions | /10 | |
| Tools and Techniques | /10 | |
| Solution | /20 | |
| Risk Analysis | /10 | |
| References | /10 | |
| **Total** | **/100** | |